

PKI Issues -- A Commercial Vendor Perspective

Dr. Roger R. Schell
Novell Corporate Security Architect
schellr@alum.mit.edu

PKI Technical Working Group (TWG)
8 July 1999 Meeting

Novell_®

Overview

- Enterprise Customer Requirements
- Common PKI Commercial Shortfalls
- Novell PKI Technology Response
- Potential DoD Applicability
- Conclusions

Enterprise Customer Technology Requirements

- Pervasive Secure Interoperability
- E-Business Capability
 - Security is Major Enabler
 - Business-to-business (B2B) E-commerce
- Able to Specify and Measure Security
- Enable Bondable/Insurable Deployment
- Simple and Effective to Manage

Enterprise Customer Business Requirements

- Liability Allocation
 - Limitation of Responsibility to What Can Be Done
 - Sufficient Resources to Permit Recovery for Damages
- Distributed Validation
 - Distribute Reliable Information In the Certificate
 - Enable Informed, Local Decisions by Relying Parties
- User Accountability
 - Ability to Constrain What Is Delegated
 - Proof of Individual Responsibility for their Actions
 - Support Non-repudiation

Common PKI Commercial Shortfalls

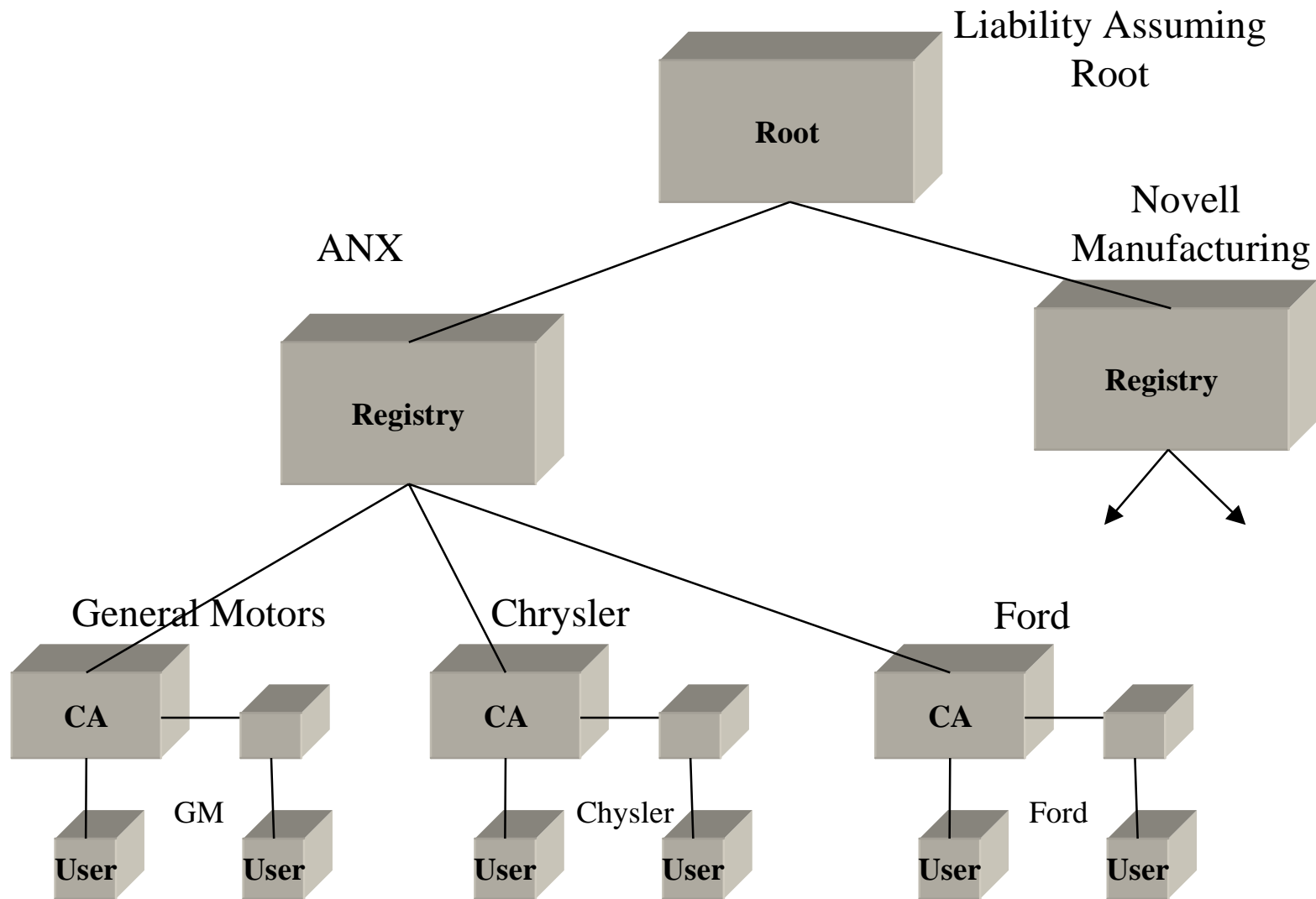
- Distorted Intermediary Liability
 - Inadequate Basis for Damage Recovery
 - Cross Certification
 - Bridge Certification Authority
- Processing of Certificate Policies
 - Name Constraints
 - OID Policy Constraints
 - Composite Impact of Entire Chain
- Vulnerability of Underlying Platforms
- Complex, Costly Management

Novell PKI Technology

Explicit Commercial Response

- Reflect Distributed Nature of Process
 - Break Tie of CA Hierarchy to Management
 - Naturally Support Many CA Servers
 - Accept Minimum of Four Level Hierarchy
- Explicit Certificate Security Quality
 - Support Cumulative Nature for Entire Chain
 - Reflect Measurable Assurance of Platform
 - Enable, not Require: non-Critical
- User Accountability Across Enterprises

Example Enterprise CA Structure



Novell PKI Technology

Reflect CA Responsibilities

- Liability-Assuming Root
 - Protect Its Private Key
 - Insure Only the Uniqueness of Registry Identity
 - Deep Pockets - for ONLY those two responsibilities
- Registries
 - Protect Their Private Key
 - Confirm (Unique) Identity of Enterprises They Register
 - May Impose Constraints on Subordinate Enterprises
- Enterprises
 - Protect Their Private Key
 - Confirm (Unique) Identity of Their Users
 - May Impose Constraints on the Properties of Their Users

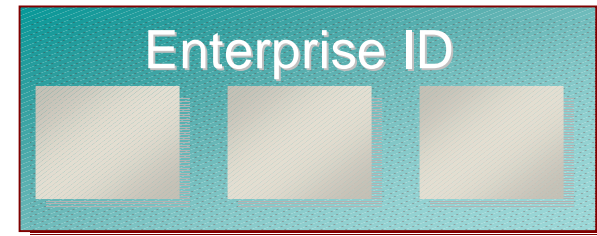
Novell PKI Technology Composite Quality Attribute



Reflects the **confidentiality** and the “**unguessability**” of the key generation used to generate the subject key of this certificate

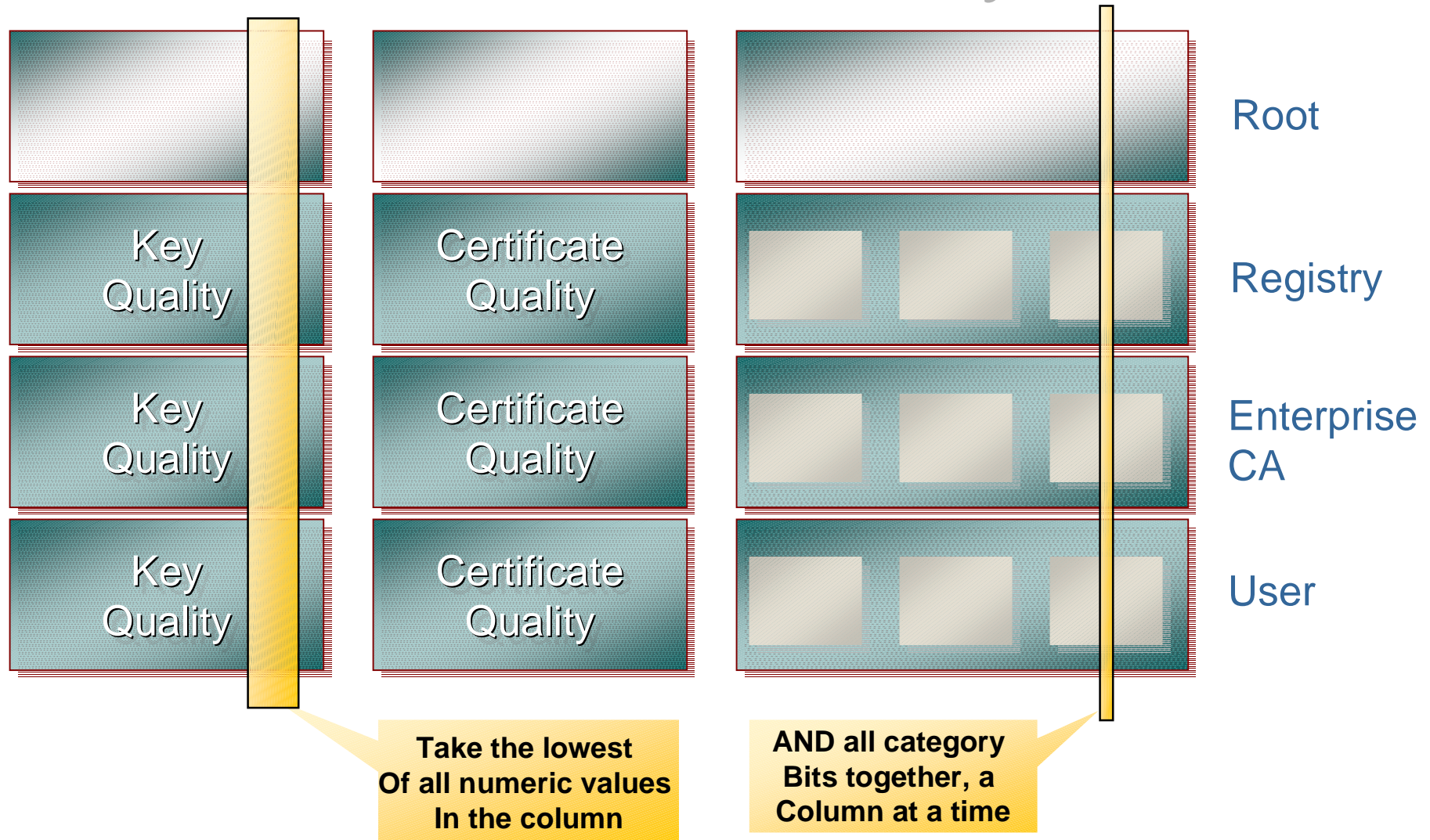


Reflects **confidence** that the certificate contents reflect the **intent** of the individual who signed this certificate



Reflects **constraints** imposed upon the identity properties of the subject of the certificate by the certificate issuer

Computing Certificate Quality Across The CA Hierarchy



Novell PKI Technology

Quality Reflects Sound Platform

- Need Measurable Assurance
 - Require High Platform and Security Expertise
 - Require Access to (Highly Proprietary) Internals
 - Need 3rd Party to Evaluate, e.g., TCSEC
- International, Modular Cryptography
- Recognizes Heterogeneous Platforms
 - Novell Registry CA Requires Wang Class B3
 - Sistex Partner Has Class C2 User Client
 - Customer NDS - Servers Can Have a CA

Novell PKI Technology

Explicit Certificate Chains

- Ubiquitous Root Interoperability
 - Shared Root Is Primary Basis, E.G., Browsers
 - Liability Assuming Root (LAR) for Business
 - Entrust, SET, Novell, Intel -- Already Responding
 - Avoids Non-extensible Stovepipe Approaches
- Discernable Certificate Quality
 - Informed Consent About Associated Liability
 - Constrained Delegation
 - Quality (Assurance) for Key and Certificate
- Wholesale Certificates Enable
 - Tension With Some Vendor Business Models

Novell PKI Technology

Simplified Management

- Exploit Novell Directory Services (NDS)
 - Widely Accessible Administration
 - Authoritative Record of User Attributes
 - Not Distant (in Time) Management
 - Reflect Business Policies
- Certificate Registry for Revocation
- “Industrial Strength” Directory
 - Scalability -- 100s of Millions of Objects
 - Security -- Access Control for Directory Objects
 - High Availability -- Writeable Replication

Potential DoD Applicability of Commercial Results

- DoD May Share Many Requirements
 - Shared Root
 - Constrained Delegation
 - Massive Scale-ability
- Optional, Application-Specific Support
 - Full Interoperability With Appropriate Security
 - Application Choice - Use When It's Needed
- Commercial Off-the-shelf Novell Products
 - World's Largest PKI Deployment - 40 Million

Conclusions

- Can Support Liability Allocation
 - Certificate Quality (trusted path)
 - Certificate Key Quality (confidentiality)
 - Trusted Platform (3rd Party Evaluation)
 - Basis for assurance for web-based services
 - Key factor in measuring certificate quality
- Can Support Individual Accountability
 - Trusted Workstation (3rd Party Evaluation)
- Can Support Distributed Validation
 - Certificate Enterprise ID
 - Ubiquitous Root Public Key